P-ISSN : 1858-3938
E-ISSN : 2721-284X

PENGUJIAN, ANALISA DAN SOLUSI PENCEGAHAN TERHADAP CELAH KEAMANAN SISTEM JARINGAN KOMPUTER STTI NIIT

Ahmad Riduan[1], Christ Evvert Lisangan[2]
[1,2]Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Informasi NIIT, Jakarta

E-mail: [1]christel@i-tech.ac.id

Abstrak

Semakin meningkatnya penggunaan teknologi jaringan komputer dan internet dalam berbagai kebutuhan namun tidak diimbangi dengan perhatian kepada sistem keamanan jaringan komputer. Jika tidak ada perhatian pada aspek keamanan tersebut maka ancaman–ancaman tindak kejahatan siber dapat terjadi. STTI NIIT memiliki infrastruktur jaringan komputer dengan media wireless (Wi-Fi) dan kabel (LAN) untuk menghubungkan berbagai perangkat dan koneksi untuk menghubungkan intranet dan internet. Dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan pengujian dan analisa terhadap celah keamanan sistem jaringan komputer yang diimplementasi STTI NIIT dari perspektif luar atau teknik Black Box Penetration Testing. Pengujian ini menggunakan metode Penetration Testing Execution Standard (PTES) yang tahapannya terdiri dari Pre-Engagement Interaction, Intelegence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting. Pengujian jaringan wireless menggunakan tools CUPP, mentalist dan aircrack-ng sedangkan pengujian jaringan LAN menggunakan Nmap untuk mencari celah keamanannya, kerentanan yang ditemukan akan dianalisa berdasarkan database Common Vulnerabilities and Exposures (CVE) dan database exploit-db untuk menemukan skrip eksploitnya. Setelah hasil pengujian dan analisa akan dilakukan tahap reporting untuk memberikan secara lengkap hasil laporan pengujian, analisa dan solusi pencegahan yang dapat dilakukan untuk menghindari serangan atau pemanfaatan terhadap celah keamanan sistem jaringan komputer yang telah diuji.

Kata kunci: Penetration Testing Execution Standard, Kerentanan, CVE

Abstract

The increasing use of computer network technology and the internet for various needs is not matched by attention to computer network security systems. If there is no attention to this security aspect, cybercrime threats can occur. STTI NIIT has a computer network infrastructure with wireless (Wi-Fi) and wired (LAN) media to connect various devices and connections to intranet and internet. In overcoming this problem, one of the steps that can be taken is to test and analyze security vulnerabilities in computer network systems implemented by STTI NIIT from an outside perspective or Black Box Penetration Testing technique. This test uses the Penetration Testing Execution Standard (PTES) method, which stages consist of Pre-Engagement Interaction, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting. Wireless network testing uses CUPP, mentalist and aircrack-ng tools while LAN network testing uses Nmap to find security holes, the vulnerabilities found will be analyzed based on the Common Vulnerabilities and Exposures (CVE) database and exploit-db database to find exploit scripts. After the results of testing and analysis, a reporting stage will be carried out to provide complete results of test reports, analysis and preventive solutions that can be implemented to avoid attacks or exploiting security vulnerabilities in computer network systems that have been tested.

***Keywords** : Penetration Testing Execution Standard, Vulnerability, CVE*

1. Pendahuluan

Dalam era modern ini masyarakat telah menikmati perkembangan teknologi khususnya di bidang informasi salah satunya yang berkembang saat ini adalah internet, dimana masyarakat memanfaatkan teknologi ini untuk kegiatan seperti mencari informasi, berbagi sumber daya data dalam satu wilayah atau beda wilayah, bertransaksi keuangan menggunakan fasilitas e-banking, serta berinteraksi sosial menggunakan layanan sosial media dan lain–lain. Dari seluruh kegiatan yang dilakukan masyarakat dalam internet perlu ada aspek-aspek yang harus diperhatikan , salah satunya

P-ISSN : 1858-3938
E-ISSN : 2721-284X

aspek keamanan dalam menggunakan internet agar tidak ada penyalahgunaan informasi, hak pengguna dan kerusakan infrastruktur.

Semakin meningkatnya penggunaan teknologi jaringan komputer dan internet dalam berbagai kebutuhan namun tidak diimbangi dengan perhatian kepada sistem keamanan jaringan komputer. Jika tidak ada perhatian pada aspek keamanan tersebut maka ancaman–ancaman tindak kejahatan siber dapat terjadi. Keamanan komputer menjadi penting karena ini berkaitan dengan data pribadi (privacy), menjaga perubahan informasi dari orang yang tidak berhak (integrity), hak akses (autentication), kerahasiaan informasi dari orang-orang yang tidak berhak (confidentiality) dan menjaga agar informasi selalu tersedia untuk diakses (availability).

Untuk mengidentifikasi, meminimalkan atau mencegah ancaman keamanan siber yang dapat menimbulkan risiko, maka perlu dilakukan pengujian terhadap risiko tersebut. Sebuah pengujian keamanan teknologi informasi adalah serangkaian kegiatan yang bertujuan untuk mengidentifikasi celah keamanan pada suatu sistem jaringan atau aplikasi. Risiko yang ditimbulkan dapat berupa pencurian informasi penting atau upaya untuk menggagalkan proses teknologi yang sedang berjalan. Kegiatan ini dipandang perlu untuk meningkatkan mekanisme perlindungan keamanan infrastruktur jaringan komputer.

STTI NIIT memiliki infrastruktur jaringan komputer dengan media wireless (Wi-Fi) dan kabel (LAN) untuk menghubungkan berbagai perangkat dan koneksi untuk menghubungkan ke internet. Pertukaran informasi yang terjadi dapat berupa informasi penting atau pribadi yang hak aksesnya hanya dapat dilakukan oleh orang-orang tertentu. Namun tidak dipungkiri bisa saja ada pihak-pihak lain yang tidak bertanggung jawab yang mencoba untuk mendapatkan akses dan menyalahgunakan informasi yang ada dan menyebabkan kerugian bagi organisasi.

Berdasarkan latar belakang masalah diatas maka dapat dijabarkan identifikasi masalah sebagai berikut:

a. Perlu adanya pengujian celah kemanan terhadap sistem keamanan jaringan komputer di STTI NIIT.
b. Bagaimana melakukan pengujian celah keamanan jaringan *wireless* (Wi-Fi) dan jaringan kabel (LAN) STTI NIIT yang berjalan saat ini serta solusi pencegahan dari hasil temuan pengujian .

Adapun tujuan yang diharapkan melakukan penelitian ini adalah:

a. Melakukan pengujian dan analisa untuk mengetahui kondisi serta melakukan pengukuran tingkat kerentanan celah keamanan sistem jaringan komputer STTI NIIT.
b. Memperoleh informasi berupa hasil pengujian pada sistem keamanan jaringan komputer STTI NIIT serta mendapatkan solusi pencegahan yang berguna sebagai bahan acuan untuk pihak kampus atau pengelola melakukan perbaikan sistem keamanan.

Menurut Sarno dan Iffano dalam (Puriwigati & Buana, 2020). Keamanan informasi merupakan upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan Anda mengoptimalkan laba atas investasi. Menurut ISO/IEC 17799:2005 dalam (Puriwigati & Buana, 2020) tentang Sistem Manajemen Keamanan Informasi, keamanan informasi berasal dari berbagai ancaman untuk menjamin kelangsungan bisnis, meminimalkan risiko bisnis, serta meningkatkan investasi dan peluang bisnis.

Menurut (Muhammad, Suwanto & Erna, 2016), *Wireless Local Area Network* (WLAN) adalah jaringan komputer yang menggunakan gelombang radio sebagai media transmisi data. Informasi (data) ditransfer dari satu komputer ke komputer lain menggunakan gelombang radio.

Menurut (Rifkie, 2018) Keamanan Jaringan atau Network Security berkaitan dengan segala aktifitas yang dilakukan untuk mengamankan network, khususnya untuk melindungi kegunaan (usability), keandalan (reliability), integritas (integrity), dan keamanan (safety) dari network dan data. Target network security adalah bagaimana mencegah dan menghentikan berbagai threats (potensi serangan) agar tidak memasuki dan menyebar pada network internal. Network security mencakup komponen hardware, software dan aturan-aturan/kebijakan keamanan jaringan.

Menurut (Quinn, 2020), pengujian penetrasi adalah proses pengujian aplikasi untuk menemukan kerentanan. Tim melakukan ini dengan mengeksploitasi jaringan dengan vektor berbahaya setelah otorisasi yang diberikan sebelumnya dari bisnis. Organisasi menyimulasikan serangan yang mirip dengan serangan nyata untuk mengidentifikasi kerentanan di semua area permukaan infrastruktur digital.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

A. Pengumpulan Data

Berikut beberapa proses yang dilalui penulis dalam pengumpulan data guna membantu dalam penulisan ini, yaitu:

P-ISSN : 1858-3938
E-ISSN : 2721-284X

1. Observasi
   Pengumpulan data dan informasi dengan cara meninjau dan melakukan pengamatan secara langsung ke objek penelitian guna memperoleh data atau gambaran serta keterangan terhadap sistem yang berjalan.
2. Studi Literatur
   Mencari pengetahuan dasar yang didapat dari buku, jurnal, artikel, internet, karya ilmiah dan media lainnya untuk melengkapi landasan teori dan sebagai acuan dasar dalam menyelesaikan penelitian ini.

B. Pengujian dan Analisa

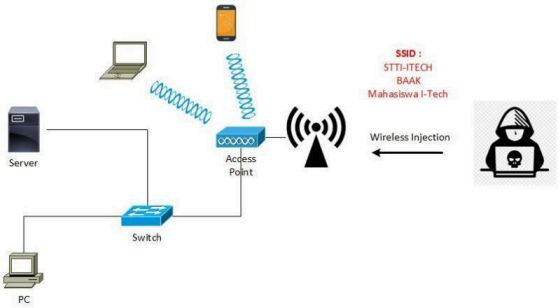
Pengujian penetrasi testing ini menggunakan teknik Black-Box penetrasi testing dengan metode Penetration Testing Execution Standard (PTES) yang tahapannya terdiri dari Pre-Engagement Interaction, Intelegence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting.

3. Hasil Penelitian dan Pembahasan

3.1. Analisa kebutuhan

Dalam analisis sistem, metode yang digunakan secara black box penetration testing yaitu di mana simulasi sebagai penyerang yang tidak memiliki pengetahuan tentang struktur internal dari sistem atau pun komponen-komponen dari target.

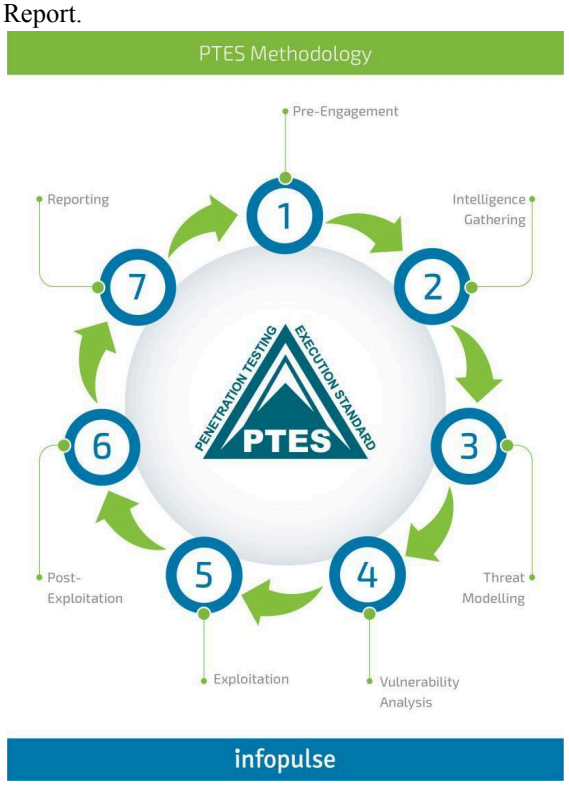
Pengujian dilakukan berdasarkan informasi yang didapat secara publik yaitu seperti sinyal Wi-Fi yang berada di kampus STTI NIIT, di mana pihak eksternal dapat melihat sinyal Wi-Fi yang di publikasikan. Penguji akan mencoba menemukan kerentanan pada jaringan wireless (Wi-Fi) menggunakan tools (alat) aircrack-ng, dan memanfaatkan kerentanan tersebut menggunakan teknik dictionary attack untuk dapat masuk ke dalam jaringan internal.



Gambar 1. Analisa Topologi Pengujian Sistem

3.2. Desain

Perancangan pengujian dan analisa pada sistem keamanan jaringan komputer STTI NIIT menggunakan metode Penetration Testing Execution Standard (PTES) yang tahapannya terdiri dari Pre-Engagement Interaction, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation dan Report.



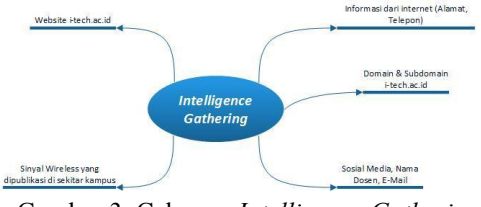
Gambar 2. PTES *Methodology*

a. Pre-Engagement Interaction

Penguji meminta izin kepada pihak kampus untuk melakukan pengujian penetrasi pada sistem target, dan pembahasan tentang ruang lingkup, waktu dan lokasi pengujian.

b. Intelligence Gathering

Mengumpulkan informasi terhadap objek atau sistem target yang akan diuji yang nantinya informasi tersebut akan digunakan untuk proses pengujian berikutnya. Beberapa contoh pengumpulan informasi dari target yaitu sinyal *wireless* yang dipublikasi, *website* dan informasi seperti alamat, nomor telepon, nama dosen, sosial media, serta informasi-informasi lainnya yang dapat dicari melalui internet.



Gambar 3. Cakupan *Intelligence Gathering*

c. Threat Modelling

Pada tahap ini, peneliti dapat menentukan model atau jenis ancaman yang memungkinkan setelah memperoleh informasi berdasarkan tahapan sebelumnya.

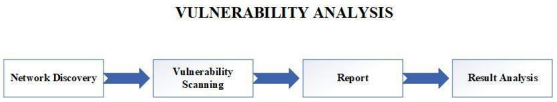
Skenario pengujian penetrasi yang dilakukan dalam penelitian ini yaitu menguji sistem

P-ISSN : 1858-3938
E-ISSN : 2721-284X

keamanan jaringan komputer STTI NIIT dimulai dari jaringan *wireless* lalu perangkat-perangkat jaringan komputer internal atau jaringan LAN dengan menggunakan *tools* uji penetrasi *aircrack-ng*, *nmap*.

d. Vulnerability Analysis

Penguji dapat menggabungkan tahapan *intelligence gathering* dan *threat modeling* untuk dapat melanjutkan ke tahap *exploitation* agar pada tahap *exploitation* dapat langsung menganalisa kerentanan (*vulnerability analysis*).



Gambar 4. Tahapan *Vulnerability Analysis*

e. Exploitation

pada tahap ini, penguji melakukan eksploitasi kepada sistem target dengan menggunakan berbagai *tools* (alat), eksploitasi ini dilakukan berdasarkan pada tahapan sebelumnya, yaitu tahap *vulnerability analysis*.

f. Post Exploitation

Setelah tahap exploitation terhadap sistem target, penguji berusaha untuk mempertahankan akses pada sistem target dan mencari target lain dari system internal yang dapat di eksploitasi dan berusaha (jika memungkinkan) untuk memiliki hak akses pada sistem target selanjutnya.

g. Reporting

Setelah pengujian penetrasi dilakukan, penguji membuat laporan terhadap hasil temuan dari pengujian tentang kerentanan yang ada pada sistem target.

3.3. Implementasi Sistem

Dari hasil yang didapatkan pada pengujian penetrasi maka langkah-langkah mitigasi/pencegahan atau solusi yang dapat diimplementasikan sebagai berikut:

a. Solusi Pencegahan Celah Keamanan Pada Jaringan Wireless

No	SSID	Jenis Serangan	Kerentanan	Solusi
	STTI-ITECH	PA2-PSK *Cracking*	Rentan terhadap *deauthenticaton attck* dan *dictionary attack* untuk mendapatkan *login password*	1. *Password* minimal 12 karakter. 2. Gunakan kombinasi huruf besar, huruf kecil, angka dan simbol. 3. Hindari *password* menggunakan kata umum dan berkaitan dengan profil pribadi. 4. Menggunakan Tipe Autentikasi WPA2 *Enterprise*

b. Solusi Celah Keamanan Pada Host Jaringan LAN

No	*Host*	Jenis Serangan	Kerentanan	Solusi
	192.168.77.28	*Denial of Service* (*Memory Consumption*)	CVE-2016-8858	*Upgrade* versi *service* OpenSSH ke versi terbaru (versi 9.1).
		Denial of Service (konsumsi CPU *crypst*)	CVE-2016-6515	
		Remote Code Execution (RCE)	CVE-2016-10009	
		Bypass IP Based Authentication	CVE-2022-31813	*Upgrade* versi *service* Apache httpd ke versi terakhir (versi 2.4.54).
		HTTP Request Smuggling	CVE-2022-22720	*Upgrade* versi *service* Apache httpd ke versi terakhir (versi 2.4.54).
	192.168.88.123	*Bypass IP Based Authentication*	CVE-2022-31813	*Upgrade* versi *service* Apache httpd ke versi terakhir (versi 2.4.54).
		HTTP Request Smuggling	CVE-2022-22720	*Upgrade* versi *service* Apache httpd ke versi

P-ISSN : 1858-3938
E-ISSN : 2721-284X

				terakhir (versi 2.4.54).

c. Solusi Pencegahan Celah Keamanan Lainnya Pada Sistem Jaringan Komputer STTI NIIT:
   1) Pembatasan lalu lintas antar segmen jaringan komputer, untuk segmen jaringan umum dan mahasiswa tidak diperbolehkan mengakses segmen jaringan yang terdapat server-server atau perangkat yang penting.
   2) Implementasi *port security* pada perangkat *switch.*
   3) Melakukan *upgrade patch OS* pada perangkat jaringan seperti *Router, Switch* dan *Access Point*.
   4) Implementasi perangkat *security* seperti *firewall* atau IPS/IDS.

4. Kesimpulan

Berikut ini adalah kesimpulan yang dapat diambil dari keseluruhan penelitian Pengujian dan Pengujian, Analisa dan Solusi Pencegahan Terhadap Celah Keamanan Sistem Jaringan Komputer STTI NIIT. Kesimpulannya adalah:

a. Implementasi pengujian ini telah mempelajari cara kerja pengujian penetrasi menggunakan teknik Black Box Penetration Testing dengan metode Penetration Testing Execution Standard (PTES) pada jaringan wireless dan jaringan LAN.
b. Hasil pengujian menunjukkan bahwa terdapat kerentanan yang telah ditemukan pada jaringan wireless dan beberapa perangkat pada jaringan LAN.
c. Hasil dari penemuan celah keamanan pada sistem jaringan komputer ini juga telah dipaparkan solusi atau pencegahannya sebagai pedoman untuk meningkatkan kualitas keamanan jaringan komputer yang berjalan saat ini.

5. Referensi

Achmady, S. (2017). Analysis Dictionary Attack dan Modifikasi Password Cracking Serta Strategi Antisipasi, 7(1), 30-37.

Andhika, Delfan, A., Slamet., Ningsih, Norma. (2022). Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES), 3(2).

Chapple, M., Stewart, James, M., Gibson, D. (2021). Certified Information Systems Security Professional Official Study Guide. USA: John Wiley & Sons.Daulay, Muhammad, I. (2019). Analisis Perbandingan Keamanan WEP, WPA, WPA2, Pada Access Point.

Fahmi, F., Abdul, F., Imam, R. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test, 8(2), 183-190.

Fauzan, Fadilla,Y., Syukhri. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang, 9(2).

Kiser, Quinn. (2020). Computer Networking and Cybersecurity.

Pratama, I Putu Agus Eka. (2015). Handbook Jaringan Komputer. Bandung: Informatika.

Primartha, Rifkie. (2018). Security Jaringan Komputer Berbasis CEH. Bandung: Informatika.

Purbo, Onno,W. (2018). Internet-TCP-IP. Yogyakarta: Andi Publisher.

Rusdan, M., Sabar, M. (2020). Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication, 2(1).

Setyawan, Muhammad, A., Raharjo, S., Kumalasari, E. (2016). Analisis Kinerja Teknologi Jaringan Wireless Pada Frekuensi 2.4 GHz Dalam Kondisi Ruangan Tertentu, 4(2), 48-62.

Sudirman, D., Yaqin, Akma, N. (2021). Network Penetration dan Security Audit Menggunakan Nmap, 7(1), 32-44.

Wicaksono, Ahmad Ismail Harry. (2018). Mendeteksi Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Komputer.

https://www.cybrary.it/blog/0p3n/using-cupp-tool-generate-powerful-password-lists/. diakses pada 13 Oktober 2020, pukul 11:47.

https://www.exploit-db.com/about-exploit-db. diakses pada 13 Oktober 2022, pukul 11:55.

https://securitytrails.com/blog/owasp-amass. diakses pada 13 Oktober 2022, pukul 12:15.

https://owasp.org/www-project-amass/. diakses pada 13 Oktober 2022, pukul 12:30.

P-ISSN : 1858-3938
E-ISSN : 2721-284X

https://www.aircrack-ng.org/doku.php. Diakses pada 15 Oktober 2022, pukul 14:30.